Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Policy on Privacy Protection

Published: 2018-06-29

© Her Majesty the Queen in Right of Canada,
represented by the President of the Treasury Board, 2018

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-24/2018E-PDF
ISBN: 978-0-660-27231-3

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Politique sur la protection de la vie privée

Policy on Privacy Protection

1. Effective date

1.1 This policy takes effect on July 1, 2018.

1.2 This policy replaces the Policy on Privacy Protection dated August 20, 2014.

2. Authorities

2.1 This policy is issued pursuant to paragraph 71(1)(d) of the Privacy Act. This policy also contains elements that relate to paragraphs 71(1)(b) and (e) of the Act.

2.2 The President of the Treasury Board, as designated Minister under the Privacy Act, is responsible for causing to be prepared and distributed policy instruments concerning the operation of the Act and its Regulations, and for prescribing forms that may be required for the operation of the Act.

2.3 The Secretary of the Treasury Board has:

2.3.1 The authority to issue, amend and rescind directives, standards and mandatory procedures, and other guidance related to this policy; and

2.3.2 Delegated authority to prescribe forms that may be required for the operation of the Privacy Act and the regulations.

3. Objectives and expected results

3.1 The objectives of this policy are:

3.1.1 To facilitate statutory and regulatory compliance, and to enhance effective application of the Privacy Act and its Regulations by government institutions;

3.1.2 To ensure consistency in practices and procedures in administering the Act and Regulations so that applicants receive assistance in filing requests for access to personal information; and

3.1.3

To ensure effective protection and management of personal information by identifying, assessing, monitoring and mitigating privacy risks in government programs and activities involving the collection, retention, use, disclosure and disposal of personal information.

3.2 The expected results of this policy are:

3.2.1 Sound management practices with respect to the handling and protection of personal information, including identifying numbers;

3.2.2 Clear responsibilities in government institutions for decision-making and managing the operation of the Privacy Act and its Regulations, including complete, accurate and timely responses to Canadians and individuals who are present in Canada and who exercise their right of access to, and correction of, their personal information under the control of government institutions;

3.2.3 Consistent public reporting on the administration of the Act through the government institution's annual reports to Parliament, statistical reports and the annual publication of Info Source, produced by the Treasury Board Secretariat (TBS); and

3.2.4 Identification, assessment and mitigation of privacy impacts and risks for all new or modified programs and activities that involve the use of personal information.

4. Requirements

4.1 Heads of government institutions are responsible for:

Delegation under the Privacy Act

4.1.1 Deciding whether to delegate, pursuant to section 73 of the Privacy Act, any of their powers, duties or functions under the Act. Careful consideration should be given as to whether a delegation should be made. The provisions of the Act containing the powers, duties or functions that may be delegated are set out in Appendix B; and

4.1.2 Signing an order, if a decision is made to delegate, authorizing one or more officers or employees of the institution, who are at the appropriate

level, to exercise or perform the powers, duties or functions of the head, specified in the order. Once an order is signed, the powers, duties or functions that have been delegated may only be exercised or performed by the head of the institution or by the named officer(s) or employee(s). Delegates are accountable for any decisions they make. Ultimate responsibility, however, still rests with the head of the government institution.

4.2 Heads of government institutions or their delegates are responsible for:

Exercising discretion

4.2.1 Exercising discretion under the Privacy Act in a fair, reasonable and impartial manner with respect to decisions made in the processing of requests and the resolution of complaints pursuant to the Act, subject to the conditions set out in the Regulation;

Privacy awareness

4.2.2 Making employees of the government institution aware of policies, procedures and legal responsibilities under the Act;

Protecting the identity of the requester

4.2.3 Ensuring that requesters' identities are protected and only disclosed when authorized by virtue of the Act and where there is a clear need to know in order to perform duties and functions related to the Act;

Processing requests

4.2.4 Directing employees of the government institution to provide accurate, timely and complete responses to requests made under the Act;

4.2.5 Implementing written procedures and practices for the government institution to ensure that every reasonable effort is made to help requesters receive complete, accurate and timely responses;

4.2.6 Establishing effective processes and systems to respond to requests for access to, and the correction of, personal information and to document

deliberations and decisions made concerning requests received under the Act;

4.2.7 Establishing procedures to ensure that:

4.2.7.1 The requested personal information is reviewed to determine whether it is subject to the Act. If subject to the Act, then determine whether any exemptions apply; and

4.2.7.2 Any consultations necessary for the processing of requests made pursuant to the Act are undertaken;

Cabinet confidences

4.2.8 Consulting departmental legal counsel, in compliance with established procedures, prior to excluding confidences of the Queen's Privy Council for Canada;

4.2.9 Acquiring in compliance with established procedures and upon the request of the Privacy Commissioner, assurances that excluded information is a Confidence of the Queen's Privy Council for Canada;

Contracts and agreements

4.2.10 Establishing measures, when personal information is involved, to ensure that the government institution meets the requirements of the Privacy Act when contracting with private sector organizations, or when establishing agreements or arrangements with public sector organizations;

4.2.11 Ensuring that appropriate privacy protection clauses are included in contracts or agreements that may involve intergovernmental or transborder flows of personal information;

Notifying the Privacy Commissioner

4.2.12 Notifying the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the Act or to any of its provisions, or that may have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved;

Use of the Social Insurance Number

4.2.13 Ensuring compliance with the specific terms and conditions related to the use of the Social Insurance Number and the specific restrictions with regard to its collection, use and disclosure;

Privacy impact assessment

4.2.14 Ensuring that, when applicable, privacy impact assessments (PIAs) and multi-institutional PIAs are developed, maintained and published;

Privacy protocol for non-administrative purposes

4.2.15 Establishing a privacy protocol within the government institution for the collection, use or disclosure of personal information for non-administrative purposes, including research, statistical, audit and evaluation purposes;

Exempt banks

4.2.16 Consulting with TBS on any proposal for the establishment or revocation of an exempt bank, and submitting a specific request to the President of the Treasury Board with regard to the proposal;

Monitoring and reporting

4.2.17 Monitoring compliance with this policy as it relates to the administration of the Privacy Act;

4.2.18 Preparing and tabling in each House of Parliament an annual report on the administration of the Act;

4.2.19 Preparing new or modified personal information bank descriptions;

4.2.20 Providing TBS with:

4.2.20.1 A copy of the annual report;

4.2.20.2 An update to its chapter in Info Source, including proposed new or modified PIBs; and

4.2.20.3

A statistical report on the administration of the Privacy Act within the institution.

4.3 The Secretary of the Treasury Board is responsible for:

4.3.1 Monitoring compliance with all aspects of this policy by analyzing and reviewing public reporting documents required by the Privacy Act and other information, such as Treasury Board submissions, Departmental Performance Reports, results of audits, evaluations and studies, to assess the government institution's administration of the Act;

4.3.2 Regularly reviewing the policy, its related directives, standards and guidelines, and their effectiveness. When substantiated by risk-analysis, TBS will also ensure that an evaluation is conducted;

4.3.3 Publishing an annual index of personal information under the control of government institutions;

4.3.4 Reviewing new and modified personal information banks, assigns a registration number to new personal information banks, and prescribes forms to be used in the administration of the Act, as well as the format and content of the annual report to Parliament;

4.3.5 Advising all members of the Access to Information and Privacy community of any updates to the policy instruments; and

4.3.6 Working closely with the Canada School of Public Service to determine the extent to which knowledge elements related to the Policy on Privacy Protection will be integrated into the required training courses, programs and knowledge assessment instruments.

5. Roles of other government organizations

5.1 This section identifies other key government organizations in relation to this policy. In and of itself, this section does not confer any authority.

5.2 The Privacy Commissioner of Canada is responsible for:

5.2.1 Investigating complaints from individuals regarding the handling of personal information by federal government institutions;

5.2.2

Conducting compliance reviews of the privacy practices of government institutions as the practices relate to the collection, retention, accuracy, use, disclosure and disposal of personal information by government institutions subject to the Act;

5.2.3 Making recommendations with respect to any matter which has been investigated or reviewed,

5.2.4 Reporting on institutional activities in annual or special reports to Parliament.

5.3 The Clerk of the Privy Council Office is responsible for determining what information constitutes a Confidence of the Queen's Privy Council for Canada.

5.4 The Department of Justice is responsible for:

5.4.1 Designating, by order-in-council, the head of a government institution for the purposes of the Act;

5.4.2 Extending the right of access by order;

5.4.3 Specifying in regulations the government institutions or part of a government institution for the purposes of subsection 3 of the Act;

5.4.4 Specifying investigative bodies;

5.4.5 Specifying persons or bodies for the purposes of paragraph 8(2)(h);

5.4.6 Specifying classes of investigations; and

5.4.7 Amending the Schedule of the Act.

6. Application

6.1 This policy and its supporting instruments apply to government institutions as defined in section 3 of the Privacy Act, including departments, ministries of state, any parent Crown corporations and any wholly owned subsidiary of these corporations.

6.2 It does not apply to the Bank of Canada.

6.3 This policy does not apply to information excluded under the Act.

7. Consequences of non-compliance

7.1 For those government institutions that do not comply with this policy, its directives and standards, TBS will require them to provide additional information relating to the development and implementation of compliance strategies in their annual report to Parliament. This reporting will be in addition to other reporting requirements and will relate specifically to the compliance issues in question.

7.2 On the basis of analysis of monitoring and information received, the designated minister may make recommendations to the head of the government institution. This could include prescribing any additional reporting requirements, as outlined in subsection 7.1 above.

7.3 The President of the Treasury Board, upon notification by TBS officials of a systemic compliance issue at a government institution, may review and revoke any delegation made under subsection 71(6) of the Privacy Act. This provision allows the President of Treasury Board to delegate to heads of government institutions that are departments as defined in section 2 of the Financial Administration Act, any of the powers, functions and duties of the designated minister with regard to the review and approval of new or modified personal information banks.

8. References

8.1 Legislation

- Access to Information Act
- Access to Information Regulations
- Canada Evidence Act
- Canadian Charter of Rights and Freedoms
- Financial Administration Act
- Library and Archives of Canada Act
- Official Languages Act
- Personal Information Protection and Electronic Documents Act
- Privacy Act
- Privacy Act Heads of Government Institutions Designation Order
- Privacy Regulations

8.2 Related policy instruments

- Directive on Privacy Impact Assessment
- Directive on Social Insurance Number
- Policy on Access to Information
- Policy on Communications and Federal Identity
- Policy Framework for Information and Technology
- Policy on Government Security
- Policy on Information Management
- Policy on Learning, Training, and Development
- Policy on Management of Information Technology

9. Enquiries

9.1 Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries regarding any questions about this policy.

9.2 Employees of federal institutions may contact their Access to Information and Privacy (ATIP) Coordinator regarding any questions about this directive.

9.3 ATIP coordinators may contact the Information and Privacy Policy Division regarding any questions about this directive.

Appendix A: Definitions

Note: Certain terms contain excerpts (in quotation marks, with the reference cited) from the Privacy Act (the Act).

administrative purpose (fins administratives)

The use of personal information about an individual "in a decision making process that directly affects that individual" (section 3). This includes all uses of personal information for confirming identity (in other words, authentication and verification purposes) and for determining eligibility of individuals for government programs.

annual report (rapport annuel)

A report submitted by the head of a government institution to Parliament on the administration of the Act within the institution during the fiscal year.

complainant (plaignant(e))

An individual who makes a complaint to the Privacy Commissioner on any of the grounds set out in subsection 29(1) of the Act.

consistent use (usage compatible)

A use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

data matching (couplage des données)

An activity involving the comparison of personal information from different sources, including sources within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Under this policy, data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

delegate (délégué)

An officer or employee of a government institution who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the Act.

designated minister (ministre désigné)

A person who is designated as the Minister under subsection 3.1(1). For the purposes of this policy, the designated minister is the President of the Treasury Board.

excluded information (renseignements exclus)

The information to which the Act does not apply as described in sections 69, 69.1, 70 and 70.1.

exempt bank (fichier inconsultable)

A personal information bank that describes files, all of which consist predominantly of personal information that relates to international affairs, defence, law enforcement and investigation, as outlined in sections 21 and 22 of the Act. The head of a government institution can refuse to disclose any personal information requested that is contained in an exempt bank.

exemption (exception)

A mandatory or discretionary provision under the Act that authorizes the head of the government institution to refuse to disclose information in response to a request received under the Act.

government institution (institution fédérale)

"Any department or ministry of state of the Government of Canada, or any body or office, listed in the schedule; and, any parent Crown corporation, and any wholly-owned

subsidiary of such a corporation, within the meaning of section 83 of the Financial Administration Act" (section 3). The term "government institution" does not include Ministers' Offices.

head (responsable)

The member of the Queen's Privy Council for Canada who presides over a department or ministry of state. In any other case, it is the person designated by the Privacy Act Heads of Government Institutions Designation Order. If no such person is designated, the chief executive officer of the government institution, whatever their title, is the head.

Info Source (Info Source)

A series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the Privacy Act. Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in Info Source PIBs, as applicable. The Info Source publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.

Implementation report (rapport de mise en oeuvre)

A notice issued by Treasury Board Secretariat to provide guidance on the interpretation and application of the Privacy Act and its related policy, directives, standards and guidelines.

multi-institutional privacy impact assessments (évaluations des facteurs relatifs à la vie privée multi-institutionnelles)

A privacy impact assessment that involves more than one government institution. (See definition of privacy impact assessment, below.)

new consistent use (nouvel usage compatible)

A consistent use that was not originally identified in the appropriate Personal Information Bank (PIB) description in the government institution's chapter in Info Source.

non-administrative purpose (fins non-administratives)

The use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistical, audit and evaluation purposes.

personal information (renseignements personnels)

"Information about an identifiable individual that is recorded in any form" (section 3). See section 3 of the Act for additional information.

personal information bank (fichier de renseignements personnels)
A description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.

privacy impact assessment (évaluation des facteurs relatifs à la vie privée)
A policy process for identifying, assessing and mitigating privacy risks. Government institutions are to develop and maintain privacy impact assessments for all new or modified programs and activities that involve the use of personal information for an administrative purpose.

Privacy Commissioner (commissaire à la protection de la vie privée)
An Officer of Parliament appointed by Governor in Council whose mission is to protect and promote privacy rights.

privacy protocol (protocol relatif à la protection des renseignements personnels)
A set of documented procedures to be followed when using personal information for non-administrative purposes including research, statistical, audit and evaluation purposes. These procedures are to ensure that the individual's personal information is handled in a manner that is consistent with the principles of the Act.

personal information request (demande de renseignements personnels)
A request for access to personal information under the Act.

program or activity (programme ou activité)
For the purposes of the appropriate collection, use or disclosure of personal information by government institutions subject to this policy, a program or activity that is authorized or approved by Parliament. Parliamentary authority is usually contained in an Act of Parliament or subsequent Regulations. Parliamentary authority can also be in the form of approval of expenditures proposed in the Estimates and as authorized by an appropriation Act. Also included in this definition are any activities conducted as part of the administration of the program.

requester (requérant)

A person who is requesting access to personal information about himself or herself or who has requested that a correction be made or a notation attached to his or her personal information.

Social Insurance Number (SIN) (numéro d'assurance sociale (NAS))
A number suitable for use as a file number or account number or for data-processing purposes, as defined in subsection 138(3) of the Employment Insurance Act. For purposes of paragraph 3(c) of the Privacy Act, the SIN is an identifying number, and is therefore considered to be personal information.

statistical report (rapport statistique)
A report that is intended to provide up-to-date statistics on the operation of the legislation. The report allows the government to monitor trends and to respond to enquiries from Members of Parliament, the public and the media. The report also forms the statistical portion of government institutions' annual report to Parliament. The forms used for preparing the report are prescribed by the designated minister, as provided under paragraphs 71(1)(c) and (e) of the Privacy Act.

Appendix B: Powers that can be delegated

Pursuant to section 73 of the Privacy Act, the head of a government institution may, by order, designate one or more officers or employees of that institution, who are at the appropriate level, to exercise or perform any of the powers, duties or functions that are to be exercised or performed by the institutional head under the following provisions of the Act and the Privacy Regulations.

Privacy Act

- 8(2)(j) Disclosure for research purposes
- 8(2)(m) Disclosure in the public interest or in the interest of the individual
- 8(4) Copies of requests under 8(2)(e) to be retained
- 8(5) Notice of disclosure under 8(2)(m)
- 9(1) Record of disclosures to be retained
- 9(4) Consistent uses
- 10 Personal information to be included in personal information banks
- 14 Notice where access requested
- 15 Extension of time limits
- 17(2)(b) Language of access
- 17(3)(b) Access to personal information in alternative format

- 18(2) Exemption (exempt bank) - Disclosure may be refused
- 19(1) Exemption - Personal information obtained in confidence
- 19(2) Exemption - Where authorized to disclose
- 20 Exemption - Federal-provincial affairs
- 21 Exemption - International affairs and defence
- 22 Exemption - Law enforcement and investigation
- 22.3 Exemption - Public Servants Disclosure Protection Act
- 23 Exemption - Security clearances
- 24 Exemption - Individuals sentenced for an offence
- 25 Exemption - Safety of individuals
- 26 Exemption - Information about another individual
- 27 Exemption - Solicitor-client privilege
- 28 Exemption - Medical record
- 31 Notice of intention to investigate
- 33(2) Right to make representation
- 35(1) Findings and recommendations of Privacy Commissioner (complaints)
- 35(4) Access to be given
- 36(3) Report of findings and recommendations (exempt banks)
- 37(3) Report of findings and recommendations (compliance review)
- 51(2)(b) Special rules for hearings
- 51(3) Ex parte representations
- 72(1) Report to Parliament

Privacy Regulations

- 9 Reasonable facilities and time provided to examine personal information
- 11(2) Notification that correction to personal information has been made
- 11(4) Notification that correction to personal information has been refused
- 13(1) Disclosure of personal information relating to physical or mental health may be made to a qualified medical practitioner or psychologist for an opinion on whether to release information to the requester
- 14 Disclosure of personal information relating to physical or mental health may be made to a requester in the presence of a qualified medical practitioner or psychologist

© Her Majesty the Queen in Right of Canada, represented by the President of the Treasury Board, 2017,
ISBN: 978-0-660-09945-3

Date modified: 2018-06-29